PROC\_USE.VULNERABLE

Ошибка "Use of vulnerable function 'String.equals()'. The standard String equality method breaks after the first character mismatch. If this method is used to work with sensitive data, it can lead to timing attacks" указывает на потенциальную уязвимость, связанную с использованием метода String.equals() для сравнения строк, особенно если эти строки содержат чувствительные данные.

Метод String.equals() в Java сравнивает символы строк поочередно от первого до последнего и возвращает false при обнаружении первого несовпадения. Однако, если строки разной длины, сравнение может быть быстрее, если первые символы совпадают.

Это поведение может быть использовано для атак типа "timing attack". Timing attack может произойти, когда злоумышленник измеряет время, затраченное на выполнение операции сравнения строк и на основе этого времени пытается вывести символ за символом содержимое строки. Такие атаки могут быть особенно серьезными, если строки содержат чувствительные данные, такие как пароли

Таблица №1 – Основные характеристики детектора PROC\_USE.VULNERABLE

|  |  |
| --- | --- |
| Категория критичности | Minor |
| Надежность | High |
| Источник | SvEng |
| Тип ошибки | Process Injection Vulnerability |
| CWE | CWE242 |
| CVE | --- |
| Возможные последствия | Выполнение произвольных команд в системе, эскалация привилегий, несанкционированный доступ к системным ресурсам |

Таблица №2 – Примеры срабатывания детектора и устранения уязвимости

|  |  |
| --- | --- |
| Потенциально небезопасное | Корректная конструкция |
| public static void incorrectTest(String command) throws IOException {  Runtime.getRuntime().exec(command); // Опасность: выполнение произвольной команды  System.out.println("Команда выполнена (небезопасно)");  } | public static void correctTest(String safeCommand) throws IOException {  // Валидация и санитизация ввода  if (!safeCommand.matches("^[a-zA-Z0-9\_.-]+$")) {  throw new IllegalArgumentException("Недопустимое имя команды");  }    // Использование белого списка разрешенных команд  if (safeCommand.equals("notepad.exe") || safeCommand.equals("explorer.exe")) {  ProcessBuilder pb = new ProcessBuilder(safeCommand);  pb.start();  System.out.println("Безопасное выполнение команды");  } else {  throw new SecurityException("Команда не разрешена");  }  } |